

WE CLAIM:

1. A smart wireless antenna subsystem, comprising:

one or more digital signal processors for controlling phases and time delays used in selectively steering a wireless radio frequency (RF) transmission beam pattern via an
5 adaptive RF beamformer;

an adaptive RF beamformer for adaptively positioning RF nulls in the wireless RF transmission beam pattern to block one or more wireless network devices from accessing a wireless network,

wherein the adaptive RF beamformer includes complex weighting factors to
10 process incoming RF signals from a plurality of wireless antenna elements and a signal weight summer to add up processed RF signals to enhance RF signals of interest and ignore RF signals not of interest;

a direction of arrival detector for computing angles of arrival of incoming RF signals from the one or more wireless network devices and for passing the computed
15 angles of arrival of the incoming RF signals to the adaptive RF beamformer; and

a plurality of wireless antenna elements for receiving a plurality of wireless RF signals from the one or more wireless network devices via the wireless network, for passing the plurality of wireless RF signals to the direction of arrival detector and for sending wireless RF signals created by adaptive RF beamformer to the one or more
20 wireless network devices.

2. The smart wireless antenna subsystem of Claim 1 wherein, the direction of arrival detector calculates a direction of arrival of an RF signal with:

$$R_{xx}(k) = E[x_k x_k^H],$$

wherein $R_{xx}(k)$ is a spatial correlation matrix, x_k is an RF signal sampled at discrete time

5 k , $E[\]$ is an expectation operator and x_k^H is a hermitian transpose of x_k .

3. The smart wireless antenna subsystem of Claim 1 wherein an output from the adaptive beamformer includes:

$$y_k = w^H \bullet x_k,$$

10 wherein y_k is an RF signal vector output at discrete time k , w^H are complex weight factors and x_k is a received RF signal vector input at discrete time k .

4. The smart wireless antenna subsystem of Claim 3 wherein the adaptive beamformer calculates the complex weight factors w^H with a Minimum Variance

15 Distortionless Response method comprising:

$$w^H = \frac{R_{xx}^{-1}(n)A}{A^H R_{xx}^{-1}(n)A},$$

wherein $R_{xx}^{-1}(n)A$ is an inverse of a spatial correlation matrix R_{xx} , n is sampled wireless signal element and A^H is a Hermitian transpose of a steering matrix.

5. The smart wireless antenna subsystem of Claim 1 wherein the smart wireless antenna subsystem is used at a physical layer in an infrastructure for the wireless network.

5 6. The smart wireless antenna subsystem of Claim 6 wherein the physical layer is an Open Systems Interconnection Layer 1 physical layer.

7. A wireless network intrusion detection and prevention system, comprising:
a plurality of monitor agent applications installed on a plurality of wireless
10 network devices for collecting wireless event data from a wireless network;
a plurality of wireless access points for providing access to the wireless network for the plurality of wireless network devices;
a secure communications link for providing secure communications between the plurality of wireless network devices and other components of the wireless network
15 intrusion detection and prevention system;
a cooperative decision engine for collecting wireless event data from the plurality of monitor agent applications installed on the plurality of wireless network devices the plurality of wireless network devices and the plurality of wireless access points, for screening the wireless event data for normal events and abnormal events, for sending
20 decision data to a response initiator adaptive feedback engine based on processing of the

normal event and abnormal events and for receiving state data from the response initiator adaptive feedback engine;

a fuzzy association engine including an adaptive learning detection system for adaptively detecting abnormal events and preventing similar abnormal events based on
5 wireless event data received from the cooperative decision engine; and

a response initiator adaptive feedback engine for receiving decision data from the cooperative decision engine, for sending state information to the cooperative decision engine, for sending response control information to a plurality of wireless access points through the secure communications link, and for maintaining a running mistrust level for
10 the plurality of wireless network devices and the plurality of wireless access points on the wireless network.

8. The wireless network intrusion detection and prevention system of Claim 7 further comprising a plurality of smart wireless antenna subsystems associated with the
15 plurality of wireless access points.

9. The wireless network intrusion detection and prevention system of Claim 8 wherein the plurality of smart wireless antenna subsystems comprise:
one or more digital signal processors for controlling phases and time delays used in
20 selectively steering a wireless radio frequency (RF) transmission beam pattern via an adaptive RF beamformer;

an adaptive RF beamformer for adaptively positioning RF nulls in the wireless RF transmission beam pattern to block one or more wireless network devices from accessing a wireless network,

wherein the adaptive RF beamformer includes complex weighting factors to
5 process incoming RF signals from a plurality of wireless antenna elements and a signal weight summer to add up processed RF signals to enhance RF signals of interest and ignore RF signals not of interest;

a direction of arrival detector for computing angles of arrival of incoming RF signals from the one or more wireless network devices and for passing the computed
10 angles of arrival of the incoming RF signals to the adaptive RF beamformer; and

a plurality of wireless antenna elements for receiving a plurality of wireless RF signals from the one or more wireless network devices via the wireless network, for passing the plurality of wireless RF signals to the direction of arrival detector and for sending wireless RF signals created by adaptive RF beamformer to the one or more
15 wireless network devices.

10. The wireless network intrusion detection and prevention system of Claim 7 wherein the secure communications link includes wireless encrypted communications.

11. The wireless network intrusion detection and prevention system of Claim 7 wherein the cooperative decision engine includes a wireless event anomaly profiler, a normal wireless event profile database and a set of wireless event misuse rules.

5 12. The wireless network intrusion detection and prevention of Claim 7 wherein the response initiator adaptive feedback engine sends alarms and wireless event log files to a network administrator, and receives manual control from the network administrator.

10 13. The wireless network intrusion detection and prevention of Claim 7 wherein the running mistrust level of the response initiator adaptive feedback engine includes a plurality of mistrust levels and a plurality of associated response mechanisms.

15 14. The wireless network intrusion detection and prevention of Claim 13 wherein the plurality of response mechanisms include a plurality of security protection suites.

15 15. The wireless network intrusion detection and prevention of Claim 14 wherein the plurality of security protection suites include an encryption method, a secure hash method, a Diffie-Hellman group method, a method of encryption key authentication and a mistrust level decrement interval.

20

16. The wireless network intrusion detection and prevention of Claim 13 wherein the plurality of associated response mechanisms includes continuing normal operation, cycling between a plurality of security protection suites, switching radio frequency bands, or excluding a wireless network device or wireless access point from the wireless network and requesting re-authentication and re-login of the wireless network device or wireless access point on the wireless network.

17. The wireless network intrusion detection and prevention of Claim 7 where the decision data includes X, Y coordinates for a physical location of a monitor agent application, wireless network or device, wireless access point where an wireless anomaly event has been detected, a confidence level in the detected wireless anomaly event, a type of wireless anomaly and a mistrust level decrement value from a security protection suite.

18. The wireless network intrusion detection and prevention of Claim 15 where a mistrust level associated with the mistrust level decrement value is calculated with:

$$M_{\text{new}} = M + \alpha\beta - M_{\text{dec_val}},$$

where M_{new} is a new mistrust level, M is an old mistrust level, α is a confidence level in a detected anomaly, β is a weight assigned to a type of anomaly and, $M_{\text{dec_val}}$ is a mistrust level decrement value.

19. An integrated wireless intrusion detection and prevention security system,
comprising:

a smart wireless antenna subsystem at a physical layer in a wireless network
5 infrastructure on a wireless network for detecting a direction of arrival of a wireless
signals from a selected wireless network device from a set of a plurality of wireless
network devices on a wireless smart antenna subsystem associated with a wireless access
point, for analyzing the direction of arrival to determine whether the detected signal is
from a rouge wireless network device, and if so, creating a wireless beamform and
10 directing the wireless signal from the rouge wireless network device to a null area in the
wireless signal pattern being transmitted by the wireless access point; and

a wireless network intrusion detection and prevention system at a data link layer
in the wireless network infrastructure on the wireless network for collecting wireless
event data from the wireless network, analyzing the collected wireless event data for
15 normal and abnormal wireless events, and for providing network security response
controls to the plurality of wireless network devices and the wireless access point on the
wireless network based on the analyzed collected wireless event data.

20. The integrated wireless intrusion detection and prevention security system of Claim 19 wherein the smart wireless antenna subsystem comprises:

one or more digital signal processors for controlling phases and time delays used in selectively steering a wireless radio frequency (RF) transmission beam pattern via an
5 adaptive RF beamformer;

an adaptive RF beamformer for adaptively positioning RF nulls in the wireless RF transmission beam pattern to block one or more wireless network devices from accessing a wireless network,

wherein the adaptive RF beamformer includes complex weighting factors to
10 process incoming RF signals from a plurality of wireless antenna elements and a signal weight summer to add up processed RF signals to enhance RF signals of interest and ignore RF signals not of interest;

a direction of arrival detector for computing angles of arrival of incoming RF signals from the one or more wireless network devices and for passing the computed
15 angles of arrival of the incoming RF signals to the adaptive RF beamformer; and

a plurality of wireless antenna elements for receiving a plurality of wireless RF signals from the one or more wireless network devices via the wireless network, for passing the plurality of wireless RF signals to the direction of arrival detector and for sending wireless RF signals created by adaptive RF beamformer to the one or more
20 wireless network devices.

21. The integrated wireless intrusion detection and prevention security system of Claim 19 wherein the wireless network intrusion detection and prevention system comprises:

- a plurality of monitor agent applications installed on a plurality of wireless network devices for collecting wireless event data from a wireless network;
- a plurality of wireless access points for providing access to the wireless network for the plurality of wireless network devices;
- a secure communications link for providing secure communications between the plurality of wireless network devices and other components of the wireless network intrusion detection and prevention system;
- a cooperative decision engine for collecting wireless event data from the plurality of monitor agent applications installed on the plurality of wireless network devices the plurality of wireless network devices and the plurality of wireless access points, for screening the wireless event data for normal events and abnormal events, for sending decision data to a response initiator adaptive feedback engine based on processing of the normal event and abnormal events and for receiving state data from the response initiator adaptive feedback engine;
- a fuzzy association engine including an adaptive learning detection system for adaptively detecting abnormal events and preventing similar abnormal events based on wireless event data received from the cooperative decision engine; and

a response initiator adaptive feedback engine for receiving decision data from the cooperative decision engine, for sending state information to the cooperative decision engine, for sending response control information to a plurality of wireless access points
5 through the secure communications link, and for maintaining a running mistrust level for the plurality of wireless network devices and the plurality of wireless access points on the wireless network.

10 22. A method for wireless intrusion detection and prevention, comprising:
detecting a direction of arrival of a wireless signal from a wireless network device on a smart wireless antenna subsystem associated with a wireless access point;
analyzing the direction of arrival to determine whether the wireless signal is from a rouge wireless network device, and if so,
15 adaptively creating a wireless beamform and directing the wireless signal from the rouge wireless network device to a null area in a wireless signal pattern being transmitted by the wireless access point.

23. The method of Claim 22 further comprising a computer readable medium
20 having stored therein instructions for causing a processor to execute the steps of the method.

24. The method of Claim 22 wherein the wireless smart antenna subsystem comprises:

one or more digital signal processors for controlling phases and time delays used
5 in selectively steering a wireless radio frequency (RF) transmission beam pattern via an adaptive RF beamformer;

an adaptive RF beamformer for adaptively positioning RF nulls in the wireless RF transmission beam pattern to block one or more wireless network devices from accessing a wireless network,

10 wherein the adaptive RF beamformer includes complex weighting factors to process incoming RF signals from a plurality of wireless antenna elements and a signal weight summer to add up processed RF signals to enhance RF signals of interest and ignore RF signals not of interest;

a direction of arrival detector for computing angles of arrival of incoming RF
15 signals from the one or more wireless network devices and for passing the computed angles of arrival of the incoming RF signals to the adaptive RF beamformer; and

a plurality of wireless antenna elements for receiving a plurality of wireless RF signals from the one or more wireless network devices via the wireless network, for passing the plurality of wireless RF signals to the direction of arrival detector and for
20 sending wireless RF signals created by adaptive RF beamformer to the one or more wireless network devices.

25. A method for wireless intrusion detection and protection security,
comprising:

maintaining plural mistrust levels for a plurality of wireless signals for a plurality
wireless network devices and for a plurality of wireless access points on a wireless

5 network by a wireless security system;

detecting a wireless signal for a wireless event for a selected wireless network
device or selected wireless access point on a smart wireless antenna subsystem;

determining a mistrust level for the detected wireless signal via the wireless
security system using decision data created on the wireless security system from the

10 detected wireless signal from the smart wireless antenna subsystem;

comparing the determined mistrust level to a mistrust level stored for the plural
wireless signals for the plural wireless network devices and plural wireless access points;
and

applying a selected security response control from the wireless security system
15 based on the determined mistrust level to selected wireless network device or wireless
access point.

26. The method of Claim 25 further comprising a computer readable medium
having stored therein instructions for causing a processor to execute the steps of the

20 method.

27. The method of Claim 25, wherein the step of determining a mistrust level includes analyzing the detected wireless signal for normal wireless events and abnormal wireless events.

5 28. The method of Claim 27, wherein the step of determining a mistrust level includes analyzing the detected wireless signal for normal wireless events and abnormal wireless events in association with an adaptive learning detection system that collects and analyzes normal wireless events and abnormal wireless events over a time period T using a neural network that is adaptively and dynamically updated based on new detected
10 wireless signals for normal wireless events and abnormal wireless events.

29. The method of Claim 25 wherein the neural network includes a Back Propagation Neural Network with positive training created with new detected wireless signal data.

30. The method of Claim 25 wherein the Back Propagation Neural Network includes a training vector:

$(SS_{C_n}, X_p, Y_p, X_{C_n}, Y_{C_n})$,

5 where SS_{C_n} a detected wireless signal strength measured at an associated wireless access point P for a selected wireless network device C_n in a particular position (X_{C_n}, Y_{C_n}) and where X_p is an X location of the selected wireless access point P, Y_p is a Y location of the selected wireless access point P and X_{C_n}, Y_{C_n} are X,Y coordinates of the selected wireless network device.

10

31. The method of Claim 25 wherein the decision data in the step of determining a mistrust level includes X,Y coordinates for a wireless network device or a wireless access point, a confidence level for the detected wireless signal, a type of wireless signal anomaly and mistrust level decrement interval from a security protection suite.

15

32. The method of Claim 25 wherein step of applying a selected security response control includes cycling among a plurality of security protection suites, switching wireless bands, requiring re-authentication and/or re-identification, forcing the selected wireless network device or wireless access point off the wireless network.

20

33. The method of Claim 32 wherein the plurality of security protection suites include an encryption method, a secure hash method, a Diffie-Hellman group method, a method of encryption key authentication and a mistrust level decrement value.

5 34. The method of Claim 25 wherein step of applying a selected security response control includes cycling among a plurality of security protection suites as mistrust level is changed for a selected wireless network device or a wireless access point based on the determined mistrust level.

10 35. The method of Claim 25 wherein step of applying a selected security response control includes directing the selected wireless network device or wireless access point to a wireless null in a wireless signal pattern with the smart wireless antenna subsystem.

15 36. The method of Claim 25 wherein the smart wireless antenna subsystem operates at physical layer in a wireless network infrastructure on the wireless network.

 37. The method of Claim 25 wherein the wireless security system operates at data-link layer or higher layers in a wireless network infrastructure on the wireless
20 network.